# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Transaksi digital adalah proses pembayaran non-tunai (*cashless*) seperti *mobile banking*, gopay, dan perangkat transaksi virtual lainnya. Fasilitas ini memudahkan orang dalam melakukan transaksi tanpa kesulitan hanya dengan menggunakan telepon seluler saja. Melalui internet pengguna dapat melakukan berbagai macam transaksi digital seperti berbelanja, *top-up*, pengiriman dana, dan masih banyak lainnya. Namun dibalik banyaknya kemudahan dan kecanggihan fasilitas yang digunakan, terdapat beberapa masalah yang terjadi. Terutama dalam hal keamanan. Hal ini dapat dilihat dari kasus kehilangan saldo gopay yang dialami oleh dua artis ternama di Indonesia yaitu Aura Kasih dan Maia Estianti. Kerugian yang dialami oleh kedua artis ternama tersebut tidak tergolong sedikit. [1]

Masalah ini menjadi hal yang perlu diperhatikan karena terbukti adanya kasus-kasus dalam industri *e-commerce* yang berkaitan dengan keamanan transaksi, mulai dari pembajakan kartu kredit, *stock exchange fraud, banking fraud*, akses ilegal ke sistem informasi (*hacking*) perusakan web sampai dengan pencurian data. Saat ini sebagian besar web atau aplikasi android yang memiliki fasilitas transaksi digital hanya menggunakan *username* atau nomor telepon dan *password* atau *pin* sebagai sarana untuk mengotorisasi pengguna agar bisa mengakses aplikasi tersebut. Apabila *username* dan *password* tersebut tercuri datanya maka hal ini akan menyebabkan sebuah kepanikan tersendiri untuk pengguna. Dari beragam kasus tersebut, maka perlu adanya sebuah perlindungan terhadap pengguna.

Beberapa perusahaan telah melakukan optimalisasi sistem keamanan transaksinya dengan menggunakan *two-factor authentication* berupa *One-Time Password*. Lalu ada juga beberapa perusahaan yang menambahkan fitur jaminan keamanan kepada pengguna, salah satunya adalah gopay dengan *gopay plus*nya. Namun, apabila para pengguna ingin mendapatkan jaminan keamanan ini perlu meng*upgrade* akun mereka menjadi gopay *plus*. Bagi sebagian pengguna hal ini cukup merumitkan karena ketentuan yang rumit seperti lulus verifikasi menjadi gopay *plus*, mengaktifkan kode *pin* sebelum kasus terjadi, dan batasan-batasan terhadap kasus yang dapat diajukan untuk pengembalian saldo. Aturan yang membatasi pengguna sehingga tidak bisa mendapatkan pengembalian saldo antara

lain:

1. Dokumentasi yang lengkap dan perlu memenuhi persyaratan.
2. Kehilangan saldo disebabkan karena kelalaian konsumen atau kasus penipuan (termasuk namun tidak terbatas pada penyalahgunaan akun yang disebabkan pemberian kode *One-Time Password* (OTP) kepada pihak ketiga manapun dan/atau melakukan pembayaran di luar aplikasi Gojek) dan/atau korban *phishing*.
3. Dan pengguna yang terindikasi dengan aktivitas mencurigakan termasuk *fraudulent behaviour/abusive behaviour/scam*/order fiktif.

Kasus yang bisa diajukan pengembalian saldo hanya jika akun pengguna diambil alih secara paksa dan atau digunakan secara tidak bertanggungjawab akibat kehilangan perangkat seluler dan saldo hilang. [2]

Oleh karena itu, faktor keamanan transaksi seperti keamanan metode pembayaran menjadi hal yang perlu diperhatikan guna memberikan kenyamanan pengguna melakukan transaksi. Maka, untuk menjamin keamanan akun pengguna yang sudah terlanjur tercuri oleh pihak lain agar tidak bisa melakukan transaksi digital, salah satunya adalah menggunakan *two-factor authentication* dengan *Challenge Response Authentication Mechanism* (CRAM). Dengan metode *two-factor authentication* ini sistem transaksi digital tidak hanya bergantung pada *username* atau nomor telepon dan *password* pengguna, tetapi juga membutuhkan apa yang dimiliki oleh pengguna yaitu token. *Time-based One Time Password* (TOTP) adalah salah satu mekanisme *two-factor authentication* dimana sandi yang dihasilkan hanya bisa digunakan satu kali dalam kurun waktu yang ditentukan.

Meskipun TOTP sudah diterapkan di beberapa aplikasi yang ada, dalam penelitian ini TOTP akan diterapkan dengan CRAM tambahan dimana kode TOTP akan diberikan kepada pengguna dengan mengakses dan melakukan validasi dari dua entitas (aplikasi dan web) dalam kurun waktu tertentu. Hal ini akan menguatkan keamanan sistem dan menyulitkan pencuri akun dalam melakukan transaksi pada akun tersebut dikarenakan banyaknya akses yang dibutuhkan dalam rentan waktu yang singkat sehingga hanya pengguna asli atau pemilik akun yang dapat melakukan transaksi digital. Contoh seperti *internet banking* dari Bank Central Asia (BCA) ketika pengguna melakukan transaksi finansial di *internet banking*, pengguna perlu melakukan *input* kode pada *key* BCA.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas, dapat diidentifikasikan masalah sebagai berikut:

1. Bagaimana cara untuk mengimplementasikan sistem otentikasi *Time-Based One-Time Password* menggunakan *challenge response authentication mechanism* untuk transaksi digital pengguna?
2. Bagaimana menguji akurasi dan penerimaan pengguna tentang sistem keamanan ini?

## 1.3 Batasan Permasalahan

Berdasarkan identifikasi masalah diatas, agar penelitian yang dilakukan menjadi lebih terarah dan tidak menyimpang dari latar belakang serta rumusan masalah yang tertera. Penulis memberikan masalah yang diambil dalam melakukan penelitian sebagai berikut:

1. Implementasi sistem otentikasi untuk melakukan transaksi digital pengguna pada aplikasi android.
2. Metode yang digunakan untuk melakukan otentikasi adalah TOTP (*Time-based One-Time Password*) dengan mekanisme *challenge response authentication* berbasis web.

## 1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini, yaitu:

1. Mengimplementasikan sistem otentikasi *Timebased One Time Password* menggunakan *challenge response authentication mechanism* berbasis web pada aplikasi Android untuk transaksi digital pengguna.
2. Menguji akurasi dan penerimaan pengguna terhadap sistem yang dibuat.

## 1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Menciptakan sistem proses otentikasi transaksi digital yang aman dengan memenuhi tiga properti keamanan sistem (*credential, integrity, & availability*).

2. Membantu mengurangi kecemasan yang dialami oleh pengguna akibat akunnya tercuri.

## 1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN
  Bagian ini menjelaskan mengenai permasalahan yang diteliti. Bagian ini terdiri dari latar belakang permasalahan, rumusan masalah, batasan permasalahan, tujuan penelitian, manfaat penelitian, dan sistematika penulisan yang digunakan dalam penelitian ini.

- Bab 2 LANDASAN TEORI
  Bagian ini menjelaskan mengenai landasan teori yang berkaitan dengan penelitian, antara lain metode Waterfall, Android, Retrofit, Firebase Authentication, Firebase Firestore Database, Node JS, React JS, Express JS, Express Rate Limiter, Crypto, One-Time Password, Hmac-based One Time Password, Time-based One-Time Password, Challenge Response Authentication Mechanism, Github, Vercel, Blackbox Testing, End User Computing Satisfaction, dan Skala Likert.

- Bab 3 METODOLOGI PENELITIAN
  Bagian ini menejelaskan mengenai metodologi penelitian yang digunakan dan diterapkan serta perancangannya, seperti analisis kebutuhan sistem, diagram alir, struktur tabel *database*, dan *mockup* aplikasi.

- Bab 4 HASIL DAN DISKUSI
  Bagian ini menjelaskan hasil implementasi dari penelitian yang dilakukan, pengujian menggunakan *Blackbox Testing*, dan hasil evaluasi berdasarkan *End User Computing Satisfaction*.

- Bab 5 SIMPULAN DAN SARAN

  Bagian ini menjelaskan kesimpulan dari penelitian yang telah dilaksanakan serta saran-saran untuk pengembangan dan penelitian-penelitian selanjutnya.